REMARKS

The Final Office Action, mailed August 18, 2009, considered claims 1-20. Claims 1-6, 9-10, 13 and 17 were rejected under 35 U.S.C. § 103 (a) as being unpatentable over Hursey et al (U.S. Publication No. 2003/0074573), hereinafter *Hursey*, in view of Marwaha (U.S. Publication No. 2004/0181685), hereinafter *Marwaha*.

By this response, claims 1, 4-5, 7-9, 12, 14-15 and 18-19 are amended, claims 2-3, 6, 10-11, 13, and 17 are cancelled, and claim 23 is newly presented, such that claims 1, 4-5, 7-9, 12, 14-16, 18-20 and 23 are pending and of which claims 1, 4-5 and 23 are the only independent claims at issue. Support for the amendments and new claim can be found throughout the specification and the previously presented claims, including but not limited to the disclosure found in paragraphs [0029]-[0033], [0054]-[0058] and Figures 2 and 6-7 of U.S. Publication No. 2005/0172338.

The present claims are generally directed to determining whether an executable script is malware according to its functionality. For example, claim 4 recites a method for determining whether an executable script is malware according to functional variables and subroutines of the script. In accordance with this method, an executable script is obtained, and a normalized signature is generated for the executable script. The normalized signature comprises normalized variables and subroutines that are normalized from corresponding variables and subroutines in the executable script. These normalized variables and subroutines are in a common format suitable for comparison to normalized signatures of known malware. The normalized variables and subroutines comprise variables and subroutines from the executable script that have been renamed according to a common naming convention. The normalized signature is compared to a normalized signature of known malware. Based on the comparison it is determined whether the executable script is malware, including determining if the normalized signature for the executable script is a complete match with a normalized signature of known malware. If it is, the executable script is reported as malware.

Claim 1 is a system claim, and claim 5 recites a tangible computer-readable medium. Claims 1 and 5 are each generally related the method of claim 4, for determining whether an executable script is malware according to functional variables and subroutines of the script. Claim 23 recites similar method, in which partial matches between the normalized signature and a malware signature are detected, and in which a second normalization and comparison occur.

Claims 1-6, 9-10, 13 and 17 were rejected under 35 U.S.C. § 103(a) as being obvious in view of *Hursey* and *Marwaha*. Claims 7-8, 11-12, 14-16 and 18-20 were objected to, but were found to

contain allowable subject matter. In view of the present amendments, Applicant respectfully submits that the independent claims are allowable over the cited references.

Hursey is generally directed to scanning compressed files for malware. Instead of uncompressing each compressed file to be scanned before comparing the uncompressed file with a malware signature (a time- and resource-intensive process), *Hursey* describes compressing the malware signatures and comparing the compressed malware signatures with each compressed file. (paragraphs [0005]-[0008]). In order to apply the correct compression algorithm to the malware signatures, *Hursey* detects the compression algorithm used on each compressed file from a header of each compressed file. (paragraphs [0009]-[0010]).

Hursey fails to disclose or suggest, among other things, *normalizing variables and subroutines from variables and subroutines in the executable script in a common format suitable for comparison to normalized signatures of known malware*, as recited by independent claims 1, 4-5 and 23, and particularly when viewed in combination with the other limitations of these claims. To illustrate, *Hursey* merely compresses the data of a malware signature, and does not normalize variables and subroutines in common format. Accordingly, *Hursey* fails at least to anticipate or render obvious this limitation.

Furthermore, *Hursey* fails to disclose or suggest, among other things, *normalized variables and subroutines comprising variables and subroutines from the executable script that are renamed according to a common naming convention*, as recited by independent claims 1 and 4-5, and particularly when viewed in combination with the other limitations of these claims. For example, *Hursey* discusses compressing malware signatures and detecting compression algorithms, but fails to rename specific elements, such as variables and subroutines. Accordingly, *Hursey* fails also to anticipate or render obvious at least this additional limitation.

Marwaha is generally directed to a common event format that includes a set of tokens, which contain information coming from different sources. In the context of an enterprise manager, a listener may receive an incoming alert message and translate the message into the common event format. (paragraph [0056]) However, *Marwaha* fails at least to overcome the foregoing deficiencies of *Hursey*. For example, *Marwaha* fails to disclose or suggest, among other things, (1) *normalizing variables and subroutines from variables and subroutines in the executable script in a common format suitable for comparison to normalized signatures of known malware,* and (2) *normalized variables*

and subroutines comprising variables and subroutines from the executable script that are renamed according to a common naming convention.

For at least the forgoing reason, independent claims 1, 4-5 and 23, as well as any corresponding dependent claims, are allowable over *Hursey* and *Marwaha*.

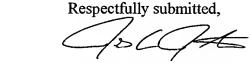
Special attention is now directed specifically to new independent claim 23, which contains additional limitations which were indicated by the Examiner to be allowable over *Hursey* and *Marwaha*. For example, claim 23 recites *generating a second normalized malware signature for the executable script ...; and comparing the second normalized signature for the executable script to second normalized signatures of know malware*...(compare to, e.g., objected to claim 14). Accordingly, claim 23 and its dependent claim, claim 12, are allowable over the cited references for at least this additional reason.

In view of the foregoing, Applicant respectfully submits that all the rejections to the independent claims are now moot and that the independent claims are now allowable over the cited art, such that any of the remaining rejections and assertions made, particularly with respect to the dependent claims, do not need to be addressed individually at this time. It will be appreciated, however, that this should not be construed as Applicant acquiescing to any of the purported teachings or assertions made in the last action regarding the cited art or the pending application and particularly with regard to the dependent claims.[1]

In the event that the Examiner finds remaining impediment to a prompt allowance of this application that may be clarified through a telephone interview, the Examiner is requested to contact the undersigned attorney at 801-533-9800.

Dated this 2nd day of November, 2009.

Respectfully submitted,



RICK D. NYDEGGER
Registration No. 28,651
JENS C. JENKINS
Registration No. 44,803
Attorneys for Applicant
Customer No. 47973

RDN:JCJ:KCC:ahy
2529595_1

[1] Instead, Applicant reserves the right to challenge any of the purported teachings or assertions made in the last action at any appropriate time in the future, should the need arise.